An Updated Survey on the IETF protocol suite for the Internet of Things

Roberto Morabito, Jaime Jiménez, Ericsson Research, Finland
{roberto.morabito, jaime.jimenez}@ericsson.com

***Abstract*—Internet of Things (IoT) is a rapidly growing technological domain and the effort that many standard organizations and alliances are dedicating to it is constantly increasing. The Internet Engineering Task Force (IETF) is certainly one of the most active standards organization operating in this broad domain. With the aim of building a comprehensive, interoperable and streamlined IoT stack, several IETF working groups are developing protocols, in multiple technological domains, which are already nowadays very relevant to the IoT. This article gives a concise but comprehensive survey of the IETF efforts in the IoT. We discuss mainstream standardization and research activities, as well as other IETF-connected supporting initiatives provided still in the context of IoT.**

I. Introduction

In the last two decades, the Internet of Things (IoT) became a significant research and development opportunity for industry, academia, and standard organizations [1]. Simplifying its definition in non-rigorous terms, IoT refers to the usage of Internet protocols for enabling communication from "things" towards humans, between "things" or more complex Internet-based infrastructures. A key aspect of the IoT is the possibility of using Internet protocol technologies on constrained devices such as sensors and actuators. Namely, devices characterized by very limited computational capabilities and that e.g. are featuring 100-250 kB in terms of max code complexity, 10-50 kB in RAM, as well as limited resources in battery, bandwidth or connectivity [2].

However, the integration of the the well-known TCP/IP Internet protocol suite [3] on top of constrained devices generates several challenges, since such protocols were not originally designed to operate along with this kind of nodes. For example, the design guidelines followed for such protocols – originally defined for the Web – may not always be suitable for network constrained environments, in which nodes are limited in CPU, memory and power and networks are often characterized by high packet loss, low throughput, frequent topology changes and small useful payload sizes [4].

The Internet Engineering Task Force (IETF) has been since long on the front line to allow overcoming such challenges, by leading the standardization of Internet communication protocols suitable for resource constrained devices and networks. Where possible, the IETF aims to make existing Internet protocols suitable for IoT scenarios, by providing minor tweaking on their definition and by taking into account the different requirements. In other cases, significant gains can only be achieved by defining new protocols.

Another key guideline followed by IETF in IoT-oriented standardization activities is the possibility of enabling a wide range of things to use interoperable technologies for communicating with each other – in this regard, "things" can range from embedded sensors to complex machinery (e.g. a car) or even large infrastructure (e.g. a bridge). As evidence of this demanded IoT interoperability, Figure 1 shows how an IoT stack deployable nowadays on constrained devices can include several IETF standards (defined for the IoT context or not), as well as Non-IETF standards.

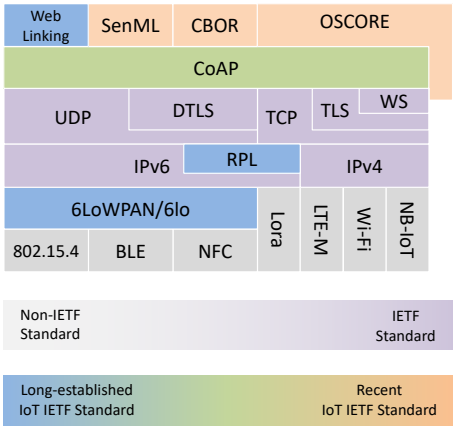

Fig. 1: An IoT stack comprising a mix of IETF and Non-IETF standards.

The above-depicted IoT stack represents just one possible example of an IoT device stack. It could easily comprise many other additional protocols, including the ones that were not originally designed for IoT or in IETF, which are now widely used in this context – e.g. the ISO standard Message Queue Telemetry Transport (MQTT) or the IETF standard HTTP. This is mainly caused by the fact that the IoT lends itself to a significant and varied number of definitions, design visions, and deployments [5].

However, since we focus on IETF and on its activities in the constrained IoT area, we rely on the vision and definition that IETF itself provides about IoT in [6]:

"The Internet of Things (IoT) refers to devices, that are often constrained in communication and computation capabilities, now becoming more commonly connected to the Internet, and to various services that are built on top of the capabilities these devices jointly provide. It is expected that this development will usher in more machine-to-machine communication using the Internet with no human user actively involved".

IETF activities are also supplemented by the Internet Research Task Force (IRTF). While the first one focuses on the shorter term matters of the Internet engineering and standards making, the second one works on longer term subjects with a clear research-oriented approach. IRTF is a much smaller organization when compared to IETF, with a substantially lower number of operating groups, called research groups.

Figure 2 illustrates different Internet-related technological meta-domains, whose development is extensively enhanced by IETF and IRTF. In the map, we identify four main areas (i.e. *Connectivity*, *Routing*, *Application*, *Security*) with which can be mapped a substantial number of IETF working groups characterized by a clear IoT scope. Additionally, several other working and research groups can somehow be classified as IoT-related, although characterized by a different general purpose. We map these additional working groups to two specific categories – *Experimental & Use Cases* and *Infrastructures*.

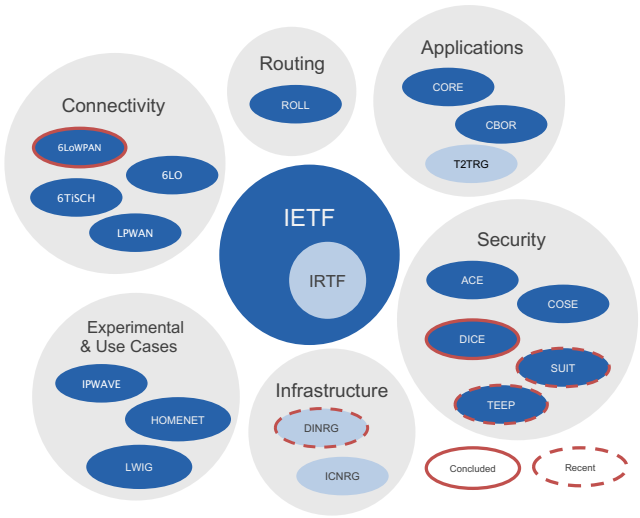

Fig. 2: IETF Working groups operating in the IoT classified in meta-domains.

The remainder of this article focuses on surveying what are the leading IETF and IRTF activities currently oriented towards the IoT in the technical domains introduced above, and it is organized as follows. We first focus on the connectivity and routing aspects. Afterwards, application and security areas are reviewed and discussed, respectively. Following, we overview ongoing standardization efforts relating to experimental activities, use cases, and infrastructures. Before the conclusion are given, we also introduce what are the other committees and organizations established to work along side with IETF and their area of responsibility in the IoT context. This article is intended to provide an update for a related work published in 2013 [7], by providing an up to date overview on the consolidated and emerging activities on IoT pursued within IETF.

Terminology. Before moving forward in our analysis, it is worth clarifying the terminology commonly used in such standardization context. The following description can help the reader familiarizing with specific terms and acronyms, which are frequently recurring in most of the IETF processes and in this article.

- *IETF Working Group (WG)* is the primary mechanism for the development of IETF specifications and guidelines, many of which are intended to be standards or recommendations.
- *IRTF Research Group (RG)* explore and work on research-related topics with a more longer-term approach when compared to a WG. However, its organizational nature remains similar.
- *Internet-Drafts (I-Ds)* are working documents of the IETF, its areas, and its Working Groups. Note that other groups may also distribute working documents as I-Ds, while I-Ds proposed in the scope of a specific WG go through an adoption process discussed within the WG itself – as opposed to individual submission I-Ds which do not require such a process.
- *Request for Comment (RFC)* is a technical and organizational publication, which describes mechanisms, implementations guidelines, or innovations applicable on topics related to Internet protocols, Internet-connected systems, applications, architecture and technology. The term ”RFC” is historically motivated as it is an archival series of publications. RFCs can follow multiple tracks; standards, informational or experimental. Standards track RFCs that are mature enough will become Proposed Standards and after they have reach a high degree of maturity and adoption they can become Internet Standards.

II. Connectivity & Routing

The IETF's work on IoT has started by bringing connectivity to the constrained space, already at the turning of this century. At that time, there were already different Wireless Sensor Networks (WSNs) proposals that were not making use of standard IETF network protocols. However, the work for connecting constrained devices to the Internet by enabling IPv6 addressing on them has represented one of the first step towards the IoT.

A. Connectivity

6LoWPAN — The IPv6 over Low power WPAN (6LowPAN) WG has operated from March 2005 to January 2014. The group produced several RFCs covering application scenarios and use cases for Low-power Wireless Personal Area Networks (LoWPANs). At that time, most of the LoWPANs were usually characterized by closed networking mechanisms, normally proprietary. Thus, the group's purpose was to bring IP, IPv6 in particular, to the short range, low bit rate, low power radios – specifically, IEEE 802.15.4 [8]. One of the big hurdles existing for enabling such integration was due to the mismatch between the maximum frame size of 127 bytes and the Maximum Transmission Unit (MTU) of IPv6. This has led to the specification of an adaptation layer that provides fragmentation and reassembly, and allows to overcome the above mentioned problem. Table 3 shows three among the most representative RFCs produced in 6LoWPAN.

6TiSCH — The WG started in 2013 and still continues. It focuses on enabling IPv6 over the Time-Slotted Channel Hopping (TSCH) MAC mode of the IEEE802.15.4 standard. The TSCH WG brings to the IoT picture the possibility of time synchronization for IoT devices, which results in less battery consumption. It is particularly targeted to industrial scenarios where interference may occur and 99.999% reliable delivery is needed. As shown in Table 3, the WG has so far focused on different aspects ranging from defining guidelines for 6TiSCH-related use cases and scenarios, to the definition of minimal IP over TSCH configuration required on a device, as well as contextualization and protocol specification for the IPv6 over the TSCH mode of IEEE 802.15.4e network – known as 6TiSCH. The group is nowadays finalizing architecture and specification of the 6TiSCH Operation Sublayer (6top) and related 6top protocol. These new specifications allow to select the appropriate Scheduling Functions (SFs), which enable the time synchronization and how node allocation and reallocation to another cell is arranged. The group is also defining the minimal requirements for a device to join the aforementioned 6TiSCH network securely. In this regard, it has prioritized the use of two CoRE WG's specification: Constrained Application Protocol (CoAP) for the messaging and Object Security (OSCORE) to secure the communication.

6Lo — Initiated in 2013, the WG has focused – like 6LoWPAN did – on bringing IPv6 connectivity over constrained node networks of different types. While 6LoWPAN was specifically for 802.15.4, 6Lo opened that focus up to other networks. They have produced guidelines for IPv6 over various constrained networks such as Bluetooth Low Energy (BLE), ITU-T G.9959 networks, Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE) or even over Master-Slave/Token-Passing (MS/TP) wired networks. The WG has also produced specifications on information and data models (e.g. MIBs for managing 6LoWPANs), adaptation layer extensions (e.g. 6LoWPAN-GHC for header compression), as well as other maintenance documents such as new IEEE Ethertype assignments, RFC updates or informational RFCs on privacy considerations. The group is still active, working on bringing IPv6 to other networks such as Near Field Communication (NFC).

LPWAN — The WG focuses on enabling IPv6 connectivity over Low Power Wide-Area Networks (LPWANs). LPWANs devices possess large coverage at the cost of substantially lower bandwidth (e.g. order of hundreds of millibits per second [9]) and reduced duty cycle. The group has selected three LPWANs to work on; Long Range (LoRa), Wireless Smart Utility Networks (WI-SUN) and Narrowband IoT (NB-IoT). The WG started its work in 2016 and has completed an overview document specification of their selected LPWAN networks. LPWAN current focus is on LPWAN Static Context Header Compression (SCHC) for CoAP and for UDP (Table 3).

B. Routing

ROLL — The Routing Over Low-power and Lossy networks (ROLL) WG focuses on routing solutions, targeting specific deployment environments such as connected home, building, and urban sensor networks. The scope of ROLL has been re-defined several times in the past. The main outcome of its earlier activities is the specifications of the RPL protocol (RFC 6550, shown in Figure 3), an IPv6 Routing Protocol for LLNs that takes into consideration various aspects including high reliability and connectivity while ensuring low resource utilization into the devices. More recently, the WG has kept maintaining and improving already developed protocols (e.g. RPL), as well as defining related extensions for routing metrics, objective functions, and multicast. Finally, the WG has also produced several documents concerning requirements and applicability statements for routing in LLNs, terminology, and security threat analysis.

Connectivity

RFC number and Title	Description
6lowpan	
RFC 4944 *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*	Describes the frame format requirements for the transmission of IPv6 packets on IEEE 802.15.4 networks. Additional aspects discussed are definition for forming IPv6 link-local addresses, provisions for packet delivery in IEEE 802.15.4 meshes, etc.
RFC 6282 *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*	Updates RFC 4944. Specifies an IPv6 header compression format for IPv6 packet delivery in 6LoWPANs. It also defines a compression mechanism for multicast addresses, as well as UDP header compression.
RFC 6775 *Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)*	This document describes simple optimizations to IPv6 Neighbor Discovery, its addressing mechanisms, and duplicate address detection for Low-power Wireless Personal Area Networks and similar networks.
6tisch	
RFC 7554 *Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement*	Describes the environment, problem statement, and goals for using the Time-Slotted Channel Hopping (TSCH) Medium Access Control (MAC) protocol of IEEE 802.15.4e in the context of Low-Power and Lossy Networks (LLNs).
RFC 8180 *Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration*	Describes the minimum requirements to enable a 6TiSCH functional network, that is how to setup a configuration for allowing IPv6 to operate over the TSCH mode of IEEE 802.15.4e. Such configuration includes baseline set of supported protocols, modes of operation, necessary bandwidth for network and security bootstrapping, etc. It also defines how IEEE Std 802.15.4 TSCH interfaces other IETF protocols.
6lo	
RFC 7428 *Transmission of IPv6 Packets over ITU-T G.9959 Networks*	Describes the frame format for transmission of IPv6 packets as well as a method of forming IPv6 link-local addresses and statelessly autoconfigured IPv6 addresses on ITU-T G.9959 networks.
RFC 7668 *IPv6 over BLUETOOTH(R) Low Energy*	Describes how low-power Bluetooth standard (version 4.0 onwards) transports IPv6 exploiting LoWPAN techniques (6LoWPAN).
RFC 8105 *Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE)*	Describes how IPv6 is transported over DECT ULE using IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) techniques.
RFC 8163 *Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks*	This specification defines the frame format for transmission of IPv6 packets and the method of forming link-local and statelessly autoconfigured IPv6 addresses on MS/TP networks.
lpwan	
RFC 8376 *Low-Power Wide Area Network (LPWAN) Overview*	Provides an informational overview of the key LPWAN technologies, which are highly considered by IETF, and analyzes their gaps for fully enable IP communication in LPWANs.
Draft Title	**Description**
6tisch	
Minimal Security Framework for 6TiSCH	Describes the steps required for a new device to securely join a 6TiSCH network. The framework involves the use of a central entity that enables the sharing of a symmetric key with the device. The framework defines the Constrained Join Protocol and its CBOR data structure, as well as configures the entire 6TiSCH communication stack for securing the device joining.
An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4	Defines the required components of a network architecture that meets the requirements of Low-Power wireless deterministic applications (e.g., low-latency, low-jitter and high-reliability packet delivery). In order to satisfy such requirements, it combines high-speed powered backbone and sub-networks using IEEE 802.15.4 TSCH.
6lo	
Transmission of IPv6 Packets over Near Field Communication	This document describes how IPv6 is transmitted over NFC using 6LowPAN techniques.
lpwan	
LPWAN Static Context Header Compression (SCHC) and fragmentation for IPv6 and UDP	Defines a framework designed for LPWAN called Static Context Header Compression (SCHC), which enables both header compression and fragmentation. It defines a header compression mechanism and its application to compress IPv6/UDP headers, as well as fragmentation and reassembly mechanism that are used to support the IPv6 MTU requirement over the LPWAN technologies.
LPWAN Static Context Header Compression (SCHC) for CoAP	Defines how to apply SCHC header compression in CoAP headers, accounting for the different CoAP (flexible) header structure when compared with IPv6 and UDP protocols.

Routing

RFC number and Title	Description
roll	
RFC 6550 *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*	Specifies an IPv6 Routing Protocol (RPL) for Low-Power and Lossy Networks (LLN), which are networks whose characterizing components (e.g. routers and interconnected devices) are constrained.

Fig. 3: Selection of relevant RFCs and I-Ds in the connectivity and routing domain.

III. Application

In the application domain, there are currently three groups between WGs and RGs that make of IoT the centre of their interest.

The Constrained RESTful Environments (CoRE) is one of the key WGs, also in view of its well-established activities started already in 2010. More recently, two additional groups have been chartered in the IoT application domain, namely the Thing-to-Thing (T2TRG) RG in 2015 and the Concise Binary Object Representation Maintenance and Extensions (CBOR) WG in 2017.

CoRE — The main goal of CoRE is to define mechanisms and frameworks that are suitable for resource-oriented applications intended to run on constrained IP networks, namely networks characterized by additional operating constraints like the one defined in ROLL and 6Lo. The Constrained Application Protocol (CoAP), which has been defined in RFC 7252, represents the foundation around which all CoRE activities are developed [10]. CoAP is an UDP-based protocol that enables manipulation of resources hosted by devices and it is considered analogous to HTTP for constrained networks. It is worth highlighting that CoAP is designed not only for being employed in constrained operating environments, but also on ordinary IP networks. On the basis of the specification of CoAP, CoRE has explored several additional aspects (e.g. security, interoperability, data sensors representation, etc.) with the purpose of building a comprehensive and standard-compliant ecosystem around it. Furthermore, it is defining several extensions for CoAP in order to supplement the protocol with additional features that make it suitable to deal with the requirements of nowadays IoT systems and applications. As an example, a more detailed explanation of group communication over IP multicast, or another where is outlined a low-complexity server-push mechanism for observing the resource state of a CoAP server (see Table 4 for more a more detailed description of RFC 7641 and others). CoAP was originally designed in order to operate over UDP and DTLS. However, CoRE is committing an increasing effort to ensure an effective mapping of CoAP towards additional transport protocols and security mechanisms (e.g. TCP and TLS in RFC 8323), application protocols (e.g. HTTP in RFC 8075), as well as not disregarding the importance of interoperability also with non-IP networks. Regarding the perspective of a larger interoperability towards non-IETF standards and implementations, CoRE is for example improving integration with the increasingly used IoT device management protocol known as Lightweight M2M (LWM2M) defined by the Open Mobile Allicance (OMA) [11]. Two concrete cases of such trend are the effort to complete the definition of the *CoRE Resource Directory*, as well as the *SenML specification* that defines an alternative representations of data format (Table 4).

CBOR — The CBOR WG has as its primary objective the maintenance of RFC 7049, which defines the Concise Binary Object Representation (CBOR) data format. Originally, CBOR was defined to make available the benefits that JavaScript Object Notation (JSON, RFC 7159) brings to the Web towards the constrained devices. CBOR includes binary data as well as an extensibility model, using a binary representation format that is easy to parse correctly. However, in view of an increasing usage as a message format in other WGs (e.g., CORE, ANIMA GRASP), the group is aiming to revise its definition and cope with existing security issues. The new CBOR definition will ensure backward compatibility, and it will be designed in such a way that a specific data definition language (CDDL, see Table 4) provides an univocal description format to express CBOR and JSON encoded messages.

T2TRG — The Thing-to-Thing Research Group (T2TRG) investigates open research questions stemming from the use of well-established standards already defined in the scope of IoT-oriented IETF WGs. It additionally explores emerging opportunities and issues arising by new requirements of IoT infrastructures, which consequently exhibit standardization potential at the IETF. It is worth clarifying that, although in this context the term ”thing” often refers to constrained nodes, this RG targets IoT architectures where not all things are highly constrained. Leaving aside the nodes' computational capabilities, it is assumed that all devices can communicate among themselves and with the rest of the Internet. As T2TRG is a research-oriented group the topics being explored vary considerably, including the management and operation of constrained-node networks, security and lifecycle management, ways to use the REST paradigm in IoT scenarios, and semantic interoperability. In Table 4, we list and describe only a very limited part of the considerable documentation produced within the T2TRG. The characteristics of the three referenced drafts show how T2TRG produces a heterogeneous style of documents, varying from State-of-the-Art analysis, advanced technical solutions, design implementation guidelines, etc. Another relevant aspect characterizing T2TRG relates to the interaction with other standardization bodies and consortia that are active in the IoT area. For example, with the W3C Web of Things (WoT) interest group [12] has been established a tight collaboration, the purpose of which is to explore how Web technologies can be harnessed in the future of IoT.

RFC number and Title	Brief summary
core	
RFC 6690 *Constrained RESTful Environments (CoRE) Link Format*	Defines a specific link format for being used by constrained web servers. The Constrained RESTful Environments (CoRE) Link Format is carried as a payload and allows describing hosted resources, their attributes, and other relationships between links.
RFC 7252 *The Constrained Application Protocol (CoAP)*	Defines the Constrained Application Protocol (CoAP), which is a RESTful application protocol mainly designed for being used in machine-to-machine (M2M) application, constrained nodes and constrained networks. Among the different CoAP features described in this document, we can find definition of the request/response interaction model between application endpoints, support for built-in discovery of services and resources, and definition of Web-related key concepts such as URIs and Internet media types.
RFC 7641 *Observing Resources in the Constrained Application Protocol (CoAP)*	Defines a CoAP extension for observing the resource state of a CoAP server. Specifically, it enables CoAP clients to be kept updated about the representation of a resource over a period of time.
RFC 8323 *CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets*	Delineates the changes required to use CoAP over TCP, TLS, and WebSockets transports.
RFC 8428 *Sensor Measurement Lists (SenML)*	Defines a format for representing simple sensor measurements and device parameters in Sensor Measurement Lists (SenML). It offers several representational notations, JSON, CBOR, EXI and XML.
Draft Title	**Description**
core	
CoRE Resource Directory	Defines an entity called Resource Directory (RD), which tries to solve the problem of direct discovery of resources hosting registrations of resources held on other servers and allowing lookups to be performed for those resources.
Object Security for Constrained RESTful Environments (OSCORE)	Defines a method for application-layer protection of the Constrained Application Protocol (CoAP), using CBOR Object Signing and Encryption (COSE). OSCORE is specifically designed for constrained environments and provides end-to-end protection between endpoints communicating using CoAP (or CoAP-mappable HTTP).
cbor	
Concise Binary Object Representation (CBOR)	Defines the Concise Binary Object Representation (CBOR) data format, which is designed to satisfy the requirements of extremely small code size, fairly small message size, and extensibility.
Concise data definition language (CDDL): a notational convention to express CBOR and JSON data structures	Defines a notational convention to express in an easy and unambiguous way structures for protocol messages and data formats that use CBOR (RFC 7049) or JSON.
t2trg	
State-of-the-Art and Challenges for the Internet of Things Security	First discusses the lifecycle stages of a thing, followed by an analysis of security threats to whom the thing may be subjected and the challenges to deal with in order to secure against these possible threats. The draft concludes with a series of recommendations to follow for the deployment of secure IoT systems.
The Constrained RESTful Application Language (CoRAL)	Defines the Constrained RESTful Application Language (CoRAL), which features a data and interaction model, but also two specialized serialization formats for the description of typed connections between resources on the Web ("links"), possible operations on such resources ("forms"), as well as simple resource metadata.
RESTful Design for Internet of Things Systems	Provides a detailed guidance for designing IoT systems that fully rely on the Representational State Transfer (REST) architectural style.

Fig. 4: Selection of relevant RFCs and I-Ds in the application domain.

IV. Security

DICE — Initiated in 2013, the DTLS In Constrained Environments (DICE) WG completed in 2016. DICE has been focusing on defining guidelines and mechanisms for the

support of Datagram Transport Layer Security (DTLS, RFC 6347) in the context of constrained environments (i.e. including constrained devices and constrained networks). Essentially, DICE provided a dedicated DTLS profile suitable for IoT applications (RFC 7925, Table 5), where CoAP is assumed to be the main protocol used to manage such resources.

ACE — The main objective of the WG is the definition of authentication and authorization mechanisms suitable for resource access in constrained environments. Three-party authentication and authorization protocols defined previously in IETF (e.g. Public Key Infrastructure – PKI, Web Authorization Protocol – OAuth) are mostly suitable for non-constrained environments and do not take into account additional requirements and limitations that IoT scenarios introduce. As an example, the need for a dynamic and lightweight access control mechanism suitable for constrained nodes, intermittent connectivity may reduce the possibility to contact an authorization server in real-time. The WG assumes that CoAP over DTLS is used to access resource-constrained servers by client devices. Table 5 describes only a very limited subset of the WG outcomes, which however allow to understand which the kind of contribution is expected by this WG. At the moment an OAuth-based framework with profiles for DTLS and OSCORE is nearing completion, while several related individual-submission I-Ds that address group communication are in the process of WG adoption.

RFC number and Title	Description
ace	
RFC 7744 *Use Cases for Authentication and Authorization in Constrained Environments*	Presents authentication and authorization mechanisms for the entire life cycle of a constrained device.
dice	
RFC 7925 *Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things*	Profiles two widely deployed Internet security protocols for IoT systems: Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) 1.2.
cose	
RFC 8152 *CBOR Object Signing and Encryption (COSE)*	Defines the CBOR Object Signing and Encryption (COSE) security mechanisms for the CBOR data format such as creation and processing of signatures, message authentication codes, representation of cryptographic keys using CBOR, etc. This specification is nowadays considered obsolete and it has been updated by new internet drafts.
Draft Title	**Description**
ace	
Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)	Defines ACE-OAuth, which is an authentication and authorization framework specially designed for constrained networks and IoT devices. The mechanism employs several building blocks including OAuth 2.0 and CoAP.
An architecture for authorization in constrained environments	Defines problem statement, terminology and an architecture for authentication and authorization in constrained-node networks, i.e. networks with constraints in terms of processing capabilities, power, communication bandwidth, etc.
cose	
CBOR Algorithms for Object Signing and Encryption (COSE)	Defines an initial set of algorithms that are used for COSE signing and encryption.
suit	
A Firmware Update Architecture for Internet of Things Devices	Defines requirements and architecture for a firmware update mechanism suitable for constrained IoT devices. The architecture is defined in such a way to decouple it from the underlying transport of the firmware images and associated meta-data.
Firmware Updates for Internet of Things Devices - An Information Model for Manifests	Defines all the information that must be present in the meta-data ("manifest") used for ensuring a secure firmware update mechanism. The manifest describes the firmware image(s) and ensures appropriate protection.
A CBOR-based Firmware Manifest Serialisation Format	Describes the format of a manifest about the firmware for an IoT device (e.g where to find the firmware, the devices to which it applies, and cryptographic information protecting the manifest).
teep	
Trusted Execution Environment Provisioning (TEEP) Architecture	Defines architecture components of a protocol for handling the lifecycle of applications running inside a Trusted Execution Environment (TEE).
The Open Trust Protocol (OTrP)	Defines the Open Trust Protocol (OTrP). The protocol is built for being suitable to the TEEP architecture and specifies message protocol for provisioning and handling applications running in a TEE.

Fig. 5: Selection of relevant RFCs and I-Ds in the security domain.

SUIT — The Software Updates for Internet of Things (SUIT) WG was chartered at the end of 2017 with the intention of mitigate IoT attacks (e.g. Mirai DDOS attack in 2017), by improving software update mechanisms. The group focuses on defining a firmware update solution that can be use with Class 1 type of devices [2], i.e., devices with 10 kB RAM and 100 kB flash. The group is currently creating a manifest format that provides meta-data about the firmware image. It also specifies pre and post conditions for the installation of the firmware as well as other parameters that need to be validated (e.g. hardware conditions, processor information, firmware makers, etc.). The intention behind the work is that the device' bootloader verifies the firmware image against the manifest before flashing the device with it. The current manifest format stems from a common information model, the WG is moving towards the adoption of a CBOR-based Manifest serialization format but it is unclear yet whether there will be just one or more different serializations of it.

TEEP — The Trusted Execution Environment Protocol (TEEP) WG was chartered in 2018. It deals with the secure area of a processor and Trusted Application (TA) components running on it. It currently contains two drafts that provide an overview of the architecture and protocol specifics. Its architecture document presents the need for an interoperable protocol for managing TAs that run in different TEEs of various devices. The document also contains definitions of the parties involved in the protocol and the requirements when it comes to TEE attestation. The group may document several attestation technologies considering different hardware capabilities, performance, privacy, and operational properties. The current protocol definition named Open Trust Protocol (OTrP) provides an RPC-like interaction with the Trusted Applications (TAs) and Security Domains (SDs).

COSE — The CBOR Object Signing and Encryption (COSE) WG was chartered in 2015 and concluded in 2016. A proposal is now to reopen it for going to full Internet Standard. The group makes use of CBOR for object signing and encryption formats. One motivation is to reuse the cryptographic keys, message authentication (MACs), encryption, and digital signatures that were done for JSON in the now concluded JOSE WG but this time in CBOR. CBOR has new capabilities that are not present in JSON, thus the intention was not to do a direct mapping from JSON to CBOR. For example as RFC 8152 mentions, COSE uses binary encoding for binary data rather than base64url, it also redefines the message structure for better identification and consistency. The group finalized the work, being that RFC 8152 its culmination.

In previous sections, we have described what is the current state-of-the-art of IETF activities that are develop new protocols and mechanisms to enable IoT networks and applications. However, the IoT standardization progress at IETF relies too on the activities of additional IETF WGs and other IETF-related organizations.

The main scope of the next sections is therefore two-fold. First, we shed light on what are the other IETF WGs and RGs whose activities, by extension, affect or consider the IoT landscape as well. Then, we briefly introduce how additional IETF committees and organizations are promoting network and infrastructure convergence also in the IoT domain.

V. Experimental, Use Cases, and Infrastructures

In the experimental and use cases domains, there are at least three WGs whose interests are closely linked to IoT.

IPWAVE — Internet protocols are playing a crucial role for the advanced deployment of modern vehicular systems, especially when considering the complex ecosystem that characterize even just one single vehicle, as well as its interactions with other network infrastructures. Within this complex context, IPWAVE WG (established in 2016) concentrates its focus on Vehicle-to-Vehicle Communications (V2V) and Vehicle-to-Infrastructure (V2I) use-cases. The main scope of the WG is to develop an IPv6 based solution to establish efficient and secure connectivity between vehicles and other infrastructure components. V2V and V2I communications may encompass the use of different link layer technologies including 802.11-OCB (Outside the Context of a Basic Service Set), 802.15.4 with 6LoWPAN, LTE-D, LPWAN, etc. Many of these link-layers already provide full support for IPv6 unlike 802.11-OCB, despite representing one of the most promising link layer in this context. In this regard, IPWAVE aims to actively coordinate with IEEE 802.11 for fully enabling transmission of IPv6 datagrams over IEEE 802.11-OCB mode. The WG also aims to document state of the art and use cases of IPv6-based vehicular networks, by taking also into account the IoT protocol suite being developed in other IETF and IRTF groups. Table 6 summarizes two I-Ds in the IPWAVE WG.

HOMENET — The Home Networking (HOMENET) WG mainly focuses on automatic configuration of IPv6 within and among home networks. The WG investigates some of the home networks setup issues that are due to use of different networking technologies by heterogeneous devices. In particular, three relevant aspects are considered. The first relates to the complexity rising by the need of managing multiple home network segments (i.e. subnets) – including scenarios in which subnets can be physically deployed in different places. These issues are, for example, generated by the concurrent use of different link layers (e.g. Ethernet technology and others designed for low-powered sensors) that require different routing and security policies. The second aspect regards the support for IPv6 in home network devices, such as gateways and routers. The use of IPv6 implies the re-definition of specific requirements and mechanisms, also on large scale when multiple gateways, routers, and subnets belong to the same home network. Such requirements include prefix configuration for routers, managing routing, name resolution, service discovery, network security. In order to satisfy the aforementioned requirements, the WG aims to define extensions and mechanisms for already existing and consolidated protocols, rather than develop new ones. HOMENET has already produced several informational and proposed standard RFCs. Table 6 summarizes two of the most relevant ones (RFC 7368 and RFC 7788).

LWIG — The main scope of the Lightweight Implementation Guidance (LWIG) WG is to provide guidelines for efficient implementation techniques and practical considerations about the usage of Internet protocols in low-capabilities devices operating in constrained environments. Defining such kind of good practices becomes crucial if we consider the limited computing power, battery capacity, available memory, or communications bandwidth of constrained (IP-capable) devices. In fact, even a minimal optimization in the software implementation and execution (even in the order of few kilobytes of code) can bring tangible benefits for reducing complexity, memory footprint, or power usage. The WG has been established with the purpose of scrutinizing several IETF protocols, some of which belong to the IoT protocol suite such as IPv6, 6LoWPAN, CoAP, and RPL. It is worth highlighting that LWIG seeks to provide recommendations for the optimization of already existing and stable protocols implementations, ensuring the critical prerequisite of preserving interoperability with other devices. Table 6 shows an RFC defining common terminology for constrained-node networks, as well as drafts outlining guidance for CoAP implementation or TCP usage guidance in IoT contexts.

RFC number and Title	Description
homenet	
RFC 7368 *IPv6 Home Networking Architecture Principles*	Describes principles, considerations, requirements and elements of a general architecture for IPv6-based home networking. Suggests how standard IPv6 mechanisms and addressing can be employed in home networking, together with the protocol extensions that are needed for ensuring additional functionality in residential home networks.
RFC 7788 *Home Networking Control Protocol*	Defines requirements for home network devices and the Home Networking Control Protocol (HNCP). HNCP provides multiple functionality such as e.g. automated configuration of addresses, name resolution, service discovery etc.
lwig	
RFC 7228 *Terminology for Constrained-Node Networks*	Defines the terminology for constrained-node networks, which is commonly used in standardization activities.
RFC 8352 *Energy-Efficient Features of Internet of Things Protocols*	Outlines the main challenges for ensuring energy-efficient protocol operations on constrained devices, together with a set of guidelines that allow overcoming such challenges. The document mainly focuses on link-layer, however, it also provides an overview of energy-efficient mechanisms available at each layer of the IETF protocol suite specified for constrained-node networks.
RFC 8387 *Practical Considerations and Implementation Experiences in Securing Smart Object Networks*	Provides an overview on the challenges that are faced for securing resource-constrained smart object devices and trade-offs generated by the use of certain security approaches. It also recommends a deployment model in which devices can signing message objects, querying about availability of suitable cryptographic libraries, and providing usage experience of those libraries.
Draft Title	**Description**
ipwave	
Transmission of IPv6 Packets over IEEE 802.11 Networks operating in mode Outside the Context of a Basic Service Set (IPv6-over-80211-OCB)	Describes the definition of key parameters for enabling an efficient transmission of IPv6 datagrams over IEEE 802.11-OCB networks. Among these parameters the supported Maximum Transmission Unit (MTU) size, the header format preceding the IPv6 header, etc.
IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases	Details problem statement and use cases on IP-based vehicular networks, considering several communications scenarios – vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X). It also analyzes proposed protocols for IP-based vehicular networking, with a particular focus on key aspects such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy.
lwig	
Building Power-Efficient CoAP Devices for Cellular Networks	Provides guidelines for the use of CoAP in the context of smart building and scenarios in which sensors communicate through cellular networks, with a special focus on optimized techniques for minimizing the power consumption.
CoAP Implementation Guidance	Provides guidelines for building lightweight implementation of CoAP.
Comparison of CoAP Security Protocols	Analyzes and compares the performance overhead of several security protocols (DTLS 1.2, DTLS 1.3, TLS 1.2, TLS 1.3, and OSCORE) when used to secure CoAP.
TCP Usage Guidance in the Internet of Things (IoT)	Provides guidelines for lightweight implementation and use of TCP in Constrained Networks. It explains several techniques to simplify a TCP stack, discussing also drawbacks.
RFC number and Title	**Description**
icnrg	
RFC 7476 *Information-Centric Networking: Baseline Scenarios*	Defines a set of scenarios that can be used as a base for the evaluation of different ICN approaches. It discusses also how ICN solutions can help satisfying general network requirements.
RFC 7927 *Information-Centric Networking (ICN) Research Challenges*	Focuses on the description of current research challenges in the ICN domain, including naming, security, routing, system scalability, mobility management, network management etc. ICN challenges in the specific context of IoT are also discussed.
Draft Title	**Description**
lcnrg	
Design Considerations for Applying ICN to IoT	Analyzes what are the main ICN characteristics that allow to cope with many of the IoT network requirements. It also discusses what are the challenges for fully enable an ICN-based IoT network.
dinrg	
Blockchain-based IoT Infrastructure Functional Requirements	Defines the functional requirements for a Blockchain-based IoT infrastructure, including the IoT device identity management, service demand and supply matching and support of smart contracts.

Fig. 6: Selection of relevant RFCs and I-Ds in the experimental and use cases and infrastructures.

Two additional IRTF research groups are showing interest on exploring the applicability of the investigated network infrastructure also to IoT scenarios: ICNRG (Information-Centric Networking) and DINRG (Decentralized Internet Infrastructure).

ICNRG — In the wide range of activities pursued by this group in the domain of Information-Centric Networking, also the IoT context is considered. RFC 7476 and RFC 7927 respectively outline what specific ICN characteristics can be exploited in IoT and what are the related research challenges that arise from such integration. To this purpose, both RFCs

provide a comprehensive literature review and analysis of ongoing research efforts that are aiming to enable such ICN-based IoT paradigm. Some of the ICN capabilities exploitable in IoT are, for example, naming, data discovery, caching, etc. However, it is also emphasized how IoT exposes all these ICN abstractions to even more strict set of requirements mainly due to the quantity of nodes, as well as type and volume of information to be processed. These two informational RFCs outline as well what have been, at the moment of their drafting, the most relevant initiatives for tackling, either full or in part, such challenges and effectively leverage ICN concepts to IoT. Table 6 further mentions two I-Ds, currently elaborated within the ICNRG, which are heavily characterized by an IoT focus. One of them describes, at a very general level, architecture design guidelines for leveraging ICN to IoT, while the other specifies dedicated mechanisms for adapting ICN to LoWPAN networks.

DINRG — The DINRG is one of the latest RG established in IRTF. Although the group has not yet produced a large number of I-Ds (and no RFC yet), its charter identifies the motivation for investigating infrastructure services that can benefit from decentralization or that are difficult to realize in connectivity-constrained networks. The connection with IoT is therefore marked with the latter mentioned aspect, as well as with the increasing awareness that centralized deployments can represent a limitation for many IoT use cases. Decentralizing infrastructure services bring additional research challenges in terms of trust management, identity management, name resolution, resource discovery etc. Such challenges are investigated by DINRG alongside with the evolution of distributed ledger technologies and the platforms that leverage them giving rise to the development of newer decentralized communication and infrastructure systems. In this regard, an I-D is currently being developed with the aim of defining the functional requirements for blockchain-based IoT infrastructure (Table 6). We are confident that DINRG will attract in the future increasingly attention, and IoT will be deemed as reference domain for this emerging research area.

VI. Supporting Organizations

IoT Directorate — The overview provided in previous sections has highlighted how, in distinct areas, IETF encompasses several WGs that highly characterize their activities looking at the IoT needs and requirements. However, beyond the activities of the WGs focusing on IoT scenarios, the entire protocol stack is evolving and many of the new technologies developed in other IETF WGs can find applicability also in IoT contexts. With a view to strengthening a fruitful coordination between WGs and external IoT standard organizations and alliances, IETF has established the IoT Directorate, an advisory group of technical experts the primary purpose of which is *"coordination within IETF on IoT-related work and increasing the visibility of IETF IoT standards visibility to other standards development organizations (SDOs), industry alliances, and other organization"* [6].

Internet Architecture Board (IAB) — The IAB is a committee established to serve and support the IETF activities, in order to facilitate the standardization process. In the specific context of IoT, IAB has organized multiple workshops (e.g., about security, architecture, and semantic interoperability [13]), with the intention of promoting IoT-related IETF activities and receive active engagement from other parties for the development of a better IoT. Furthermore, it has also drawn up an informational document that offers guidance for designing Internet-connected smart objects networks [14].

Internet Assigned Numbers Authority (IANA) — IANA is an organization that coordinates and manages domain names (e.g. through DNS Root), IP addressing, as well as maintaining the Internet protocols numbering systems where e.g. protocols parameters specified in RFCs are defined. IANA is responsible of assigning and registering the static fields defined in the different protocols. In the case of IoT, several protocol constants require a well-kept registry (e.g. CoAP Content-Formats, COSE Algorithms, 6LoWPAN Capability Bits, or CBOR Tags), which is regularly defined during the publication of new RFCs [15].

VII. Conclusion

The IETF is a leading entity for specification and documentation of key IoT standards, as well as guidelines for its implementations. Its focus on IoT is constantly growing, besides strengthened by a larger adoption of the IETF IoT accross other standards development organizations (SDOs). Furthermore, the focus given to IoT is constantly growing and being strengthened by a larger adoption of the IETF IoT stack across organizations and consortia. The main goal of this article was to provide a comprehensive and detailed overview on the current IETF activities in support of IoT deployments. We have inspected six meta-domains, presenting what is the main focus of the different IETF-related groups operating in each single area. We have also presented a concise summary of the main outcomes – RFCs – produced by the working groups, as well as some of the most significant technical areas currently explored – relevant I-Ds.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] C. Bormann, M. Ersue, and A. Keranen, "RFC7228 – Terminology for Constrained-Node Networks," May 2014. [Online]. Available: http://tools.ietf.org/rfc/rfc7228.txt

[3] B. A. Forouzan and S. C. Fegan, *TCP/IP protocol suite*. McGraw-Hill Higher Education, 2002.

[4] I. Ishaq, D. Carels, G. Teklemariam, J. Hoebeke, F. Abeele, E. Poorter, I. Moerman, and P. Demeester, "IETF Standardization in the Field of the Internet of Things (iot): a Survey," *Journal of Sensor and Actuator Networks*, vol. 2, no. 2, pp. 235–287, 2013.

[5] R. Minerva, A. Biru, and D. Rotondi, "Towards a Definition of the Internet of Things (IoT)," *IEEE Internet Initiative*, vol. 1, pp. 1–86, 2015.

[6] "IETF – Internet of Things," https://www.ietf.org/topics/iot/, accessed: 2018-12-08.

[7] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung, "A Survey on the IETF Protocol Suite for the Internet of Things: Standards, Challenges, and Opportunities," *IEEE Wireless Communications*, vol. 20, no. 6, pp. 91–98, 2013.

[8] I. W. Group *et al.*, "Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks," *IEEE Standard*, vol. 802, no. 4, p. 2003, 2003.

[9] C. Gomez, J. Paradells, C. Bormann, and J. Crowcroft, "From 6lowpan to 6lo: Expanding the universe of ipv6-supported technologies for the internet of things," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 148–155, Dec 2017.

[10] C. Bormann, A. P. Castellani, and Z. Shelby, "Coap: An application protocol for billions of tiny internet nodes," *IEEE Internet Computing*, vol. 16, no. 2, pp. 62–67, March 2012.

[11] "Lightweight M2M (LWM2M) – OMA Specworks," https://www.omaspecworks.org/what-is-oma-specworks/iot/lightweight-m2m-lwm2m/, accessed: 2018-12-08.

[12] "Web of Things Interest Group," https://www.w3.org/WoT/IG/, accessed: 2018-12-08.

[13] J. Jimenez, H. Tschofenig, and J. Arkko, "Report from the Internet of Things (IoT) Semantic Interoperability (IOTSI) Workshop 2016," https://datatracker.ietf.org/doc/rfc8477/, Tech. Rep., 2016.

[14] H. Tschofenig, J. Arkko, D. Thaler, and D. McPherson, "Architectural Considerations in Smart Object Networking," Tech. Rep., 2015.

[15] "IANA – Protocol Registries," https://www.iana.org/protocols/, accessed: 2018-12-08.